All Sessions Outcome

ITU Workshop on 5G Security

Geneva, Switzerland, 19 March 2018

Session 1: Understanding threats and security requirements of 5G

Takeaways and Conclusions

1. Identified 5G security topics, such as threats, requirements, vison, architecture, etc.
2. Identified differences between LTE and 5G (Network architecture, Data speed/Latency/Massive Connectivity) , and related security requirements.
3. 5G security framework (architecture, radio, virtualization, ID management, energy efficient security, security assurance).
4. Application security topics.

Suggestions to ITU-T SG17

- ❑ ITU-T can contribute to 5G security, because there are many kinds of security topics that should be resolved.
- ❑5G architecture can mitigate cyber attacks. This is a chance to harden the network infrastructure.
- ❑Close collaboration with many stakeholders is required to keep the security in 5G network.
- ❑Prioritize is important to study 5G security in ITU-T.

Session 2: Overview of 5G security

Takeaways and Conclusions

1. NGMN SCT is taking a holistic 5G security approach, interacting with standardization and other relevant organizations.
2. ITU-T SG13 is home to Trust standardization, which should also be taken into account by 5G network.
3. Next phase 5G standard expects to contain more security features, specifically new authentication and data protection scheme for massive IoT devices.
4. Overview of major changes in 5G security architecture and procedures.

Suggestions to SG17

- ❑ to coordinate with NGMN SCT and other SDOs on 5G security standardization.
- ❑ to consider Trust as an important item for 5G security standardization.
- ❑ to identify new security schemes for massive IoT devices in next phase 5G standard.
- ❑to coordinate with 3GPP SA3 on 5G security standardization.

Session 3: Mitigating security threats to 5G

Takeaways and Conclusions

1. Operators already understand 5G Security issues and significant standardization gap urgency for 5G Security.
2. Trust model evolved from one extreme (completely trusted) to another one (completely distrusted) over two decades, yet the number of constituencies increased by an order of magnitude in quality and a large multiplier effect in volume and trust will require a lot of conditions to be programmatically implementable.
3. It is impossible to address 5G Security without understanding the new ecosystem impact and the new onboarding issues regarding security and privacy with its associated required and evolving compliancy requirement framework.
4. Threat landscape for 5G Security can be systematized and categorized with many lessons from the past already.
5. Academia produced very good solution architecture analysis and mitigation work regarding 5G Security including reference architectures based on OAI with concrete Proof of Concepts.

Suggestions to ITU-T SG17

- ❑ There are still significant 5G Security standardization gaps, both significant and urgent to be addressed and SG17 is plainly in its role here.
- ❑ Several topics for 5G Security Standardization emerged already:
  - ❑ 5G Security requires an explicit Security Orchestrator for End to End Hybrid architecture, in particular but not only for SDN and NFV. OAI can help approach Reference Architecture
  - ❑ The opportunity to revisit X.509 and PKI infrastructure to be powered by DLT as already started in Q14 X.ss-dlt
  - ❑ A minimum requirement for compliancy framework for operators ‘a la’ X.sup-myuc
  - ❑ Many other topics: Architecture, Quantum, IDM, Big Data, Service/Application layer and deal with pervasive encryption, etc.
  - ❑ A need to distinguish Security for 5G vs Security from 5G (perhaps a new instance from X.tfss for 5G Security in Q7/17?)
- ❑ Trust needs to be studied but it should be clearly with a long term goal as many foundations are missing.
- ❑ As already discovered in previous SG17 meeting, ecosystems must be defined and way beyond SG17 and should be handled across at least ITU-T and brought to TSAG with a Liaison Statement.
- ❑ Threat landscape can be systematically covered for 5G.
- ❑ SG17 should consider hire new researchers from academia.

Session 4: Panel discussion – Future directions on 5G security standardization activity

Takeaways and Conclusions

1. Identified standardization groups related to 5G security: NGMN Security Competence Team (SCT), 3GPP SA3, ETSI ISG NFV, GSMA, OASIS, and others (for example, IETF I2NSF, TLS, QUIC, UTA).

2. Identified SGs in ITU-T: SG11, SG13(to take the lead on 5G), SG15(transport), SG17(security aspects), Joint Coordination Activity on IMT2020 (JCA-IMT2020) under SG13, and FG-ML5G.

Suggestions to ITU-T SG17

❑ Collaborate with relevant groups and participate in JCA on IMT2020 for 5G security standardization work.

❑ Develop a standardization roadmap for 5G security and identify gaps for SG17 to study in the area of 5G security.

❑ Utilize trust model by 3GPP as a starting point.

❑ Study minimum compliance risks related to 5G applications.

❑ Utilize the cloud, big data and SDN infrastructure to build 5G security infrastructure.

Session 4: Panel discussion – Future directions on 5G security standardization activity

Takeaways and Conclusions

3. Identified security subjects: Security for network slicing, NFV/SDN and Edge computing.
4. Relevant Questions in SG17:Q4/17, Q9/17, Q11/17 (General issues), Q2/17(network aspects), Q6/17(infrastructure aspects), Q7/17(application aspects), Q8/17 (cloud computing security), Q11/17 (Cryptographic algorithm aspects), and Q14/17 (DLT).
5. Use multiple relevant Questions in SG17
6. Take an orchestrated security and holistic security approach.

Suggestions to ITU-T SG17

❑ Study security for network infrastructure, edge cloud computing, end-to-end, and cryptographic profile: for example, security orchestration, trust concept and trust model based on PKI, DLT based PKI, IDM for 5G, multi-level certification, quantum aspects, management automation aspects using AI and machine learning, and DLT-based management.

❑ Ask members to submit Contributions for 5G security.

❑ Ask relevant Questions to identify appropriate work items for 5G security.